从委内瑞拉全国大停电事件看电力关键信息基础设施安全建设

3 月 7 日，委内瑞拉遭遇了一场全国范围内的大停电，这场停电导致了该国包括首都加拉加斯在内的 20 个州失去电力供应，要知道该国一共只有 23 个州。这次停电长达 9 小时，不仅影响了通信网络，还引发了连锁效应，由于停电，卫生工作者组织报告医院有 80 多人因停电而死亡。委内瑞拉总统马杜罗更指出这是美国人发起的“电战”。

国土空间安全有军队保护，网络空间由谁保护？现实情况是我国的绝大多数工业控制系统网络安全（简称工控网络安全）几乎零保护！

工控网络安全（关键信息基础设施安全） = 国家安全，希望大家摒弃侥幸心理，务必重视，务必加紧建设工控网络安全。

委内瑞拉大停电事件再次为我们敲起警钟！！！

一、委内瑞拉大停电事件回顾

”瀑布之国“---委内瑞拉电力系统主要依靠水电，拥有装机 1006 万千瓦、发电量达 510 亿千瓦时的全球第四大水电站古里水电站。3 月 7 日下午 4 点 50 分，该水电站遭受网络攻击，导致几乎整个委内瑞拉电网瓦解，委内瑞拉大部分地区陷入黑暗之中，导致全国交通瘫痪、医院手术中断、所有通讯线路中断。3 月 8 日和 3 月 9 日的供电恢复过程中，该国再次遭受持续性的“高科技手段”实施的电磁攻击。关于此次事件，委内瑞拉总统马杜罗说：

"我国电力系统已成为最新一轮'网络攻击'的目标。"

“我们在中午又受到了一次攻击……干扰了重新连接（电力系统）的过程，到中午之前所有的系统都瘫痪了。”

这就是国家安全战争！

事件发生过程中，委内瑞拉并没有披露具体的攻击过程，与其说他没有披露，不如说他**尚没有充分的技术手段监测攻击过程，更没有工控网络安全产品保护他们的电力系统。**也许攻击者的眼睛正盯着他们水电站的漏洞，准备下一次的、任意的网络攻击……

二、电力行业工业控制系统现状

1. 电力行业一般包括发电、输电、变电、配电四个环节，其中每个环节都会采用工控系统，包括 PLC、DCS、SCADA 等，这些系统均存在**大量的已知漏洞和未知漏洞。**

2. 美国工业与安全局(BIS)公布**“瓦森纳协定”**限制黑客技术全球贸易。ICS 漏洞武器化正式开始。

3. 我国《工业控制系统信息安全行动计划（2018-2020）》指出我国**工控安全全面面临安全漏洞不断增多**、安全威胁加速渗透、攻击手段复杂多样等新挑战。

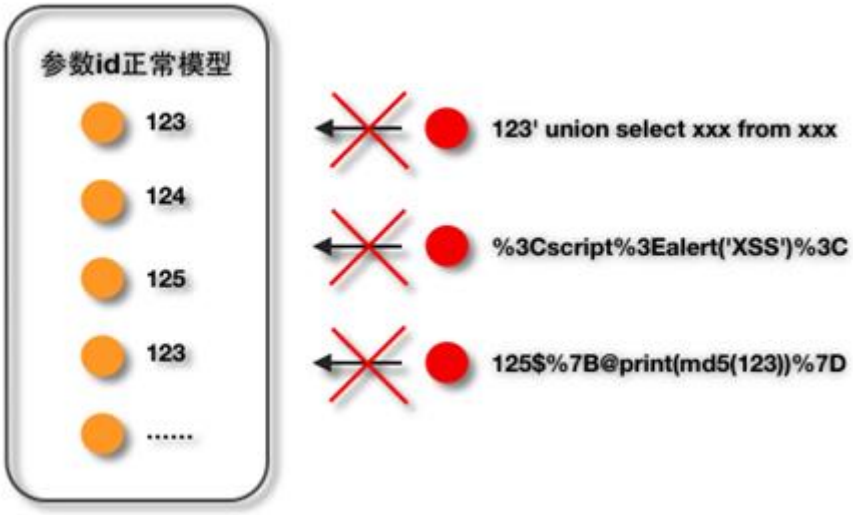
4. 未知漏洞（0DAY 漏洞）一直是**网络安全难题，尤其是在工控系统。**

5. ICS 系统间接联网，**在线更新入侵特征库难以实现。**

电力行业未知威胁防护呼之即出！

三、六方云技术储备之-AI 防御未知威胁

有别于基于特征检测、只能检测到库文件中已有威胁的“静态检测”的防火墙，**基于机器学习的自适应异常行为分析**，是一种检测未知威胁的新型技术，它是通过不断收集历史流量数据，建立流量和行为模型的一种**“动态检测”**技术。



如果我们能够搜集大量参数 ID 的正常参数值，建立起一个能够表达所有正常值的正常模型，那么一切不满足于该正常模型的参数值，即为异常。

机器学习技术可以通过对流经设备的流量进行连续、实时监控来分析流量信息，利用统计分析、关联分析和机器学习等多种技术手段建立流量和用户或应用行为中的行为正常模型，并以此模型发现异常行为。

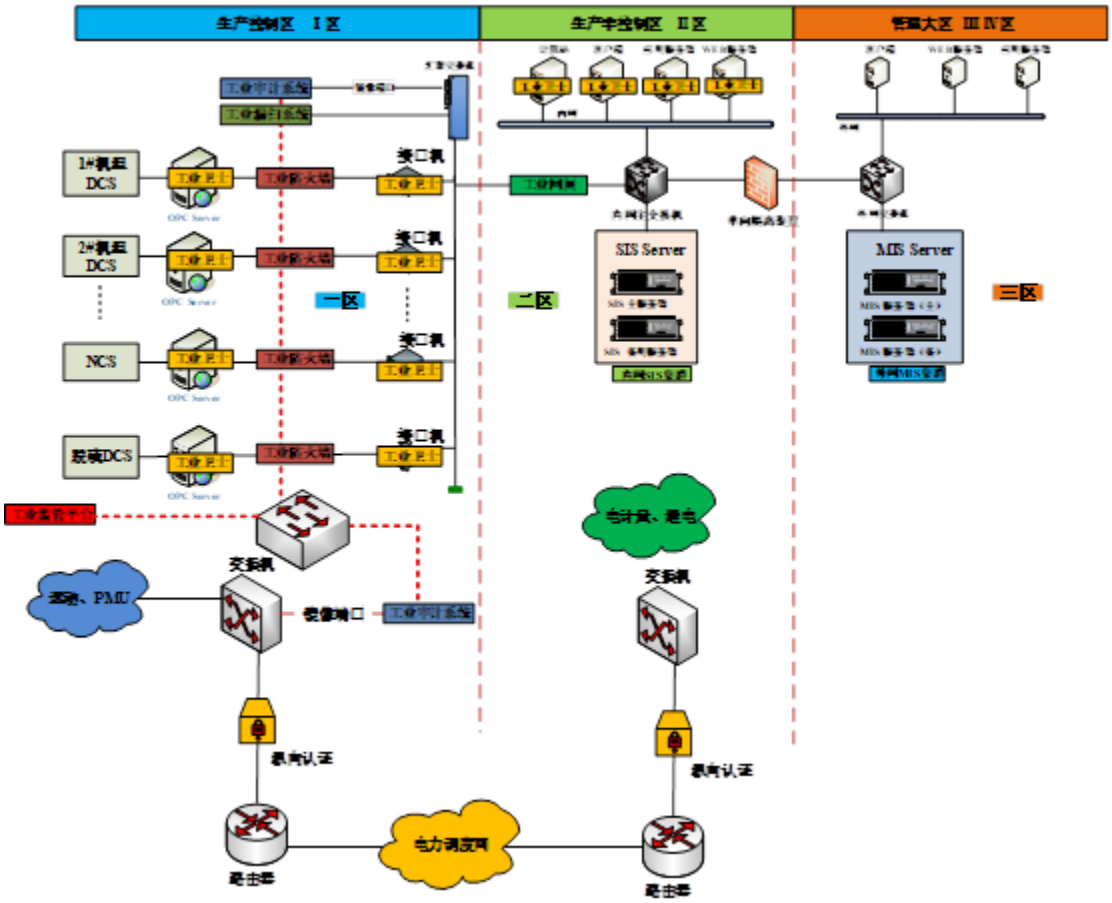
六方云 AI 防御未知威胁具有如下优势：

1. 自我进化能力
2. 借助机器学习和 AI 算法，威胁检测更全面、更准确
3. 不依赖先验知识，有效检测未知安全威胁

四、电力系统整体解决方案

水利发电行业作为国家重要的关键基础设施，为工业生产和经济发展做出巨大贡献。水电工业信息系统主要包括工业控制系统和信息管理系统两大部分；水电工业信息网络一般分为三个区域，分别为生产控制 I 区、生产非控制 II 区和管理大区。随着信息技术、通信技术的发展，工业控制系统由原来相对封闭、稳定的环境变得更加开放和多变，安全事件频发。

解决方案



1、工业主机保护

工业控制系统主机、电厂信息管理系统主机及服务器、网络边界通信网关、Web 服务器等部署**工业卫士**，确保被保护主机只有白名单规则内的程序、进程才允许运行，防止已知和未知恶意程序的侵入，进而防止电厂信息系统被恶意破坏。

2、边界安全保护&关键设备防护

生产控制 I 区、生产非控制 II 区和管理大区工业控制系统、SIS（厂级信息监控系统）之间部署**工业防火墙（或工业网闸）**。生产控制 I 区内部的锅炉、汽机等工业控制系统控制器前端布置**终端工业防火墙**。

工业防火墙对工业协议机器进行智能学习、深度数据包解析，通过白名单、黑名单、IP/MAC 地址绑定方式保护电厂信息系统。

3、工业审计

生产控制 I 区、生产非控制 II 区和管理大区电厂信息系统**旁路**布置**工业审计**产品，实现对 DCS、PLC、SIS 网络流量数据的实时监控、实时告警、行为安全审计、非法操作识别、异常事件记录、外部攻击分析等。

4、内网威胁管理

对工业安全防护设备及软件进行监控、配置、升级，进而对工业网络进行安全风险分析和风险事件智能化显示，构建持续性的威胁监视、管控机制。

五、总结

没有关键信息基础设施的安全，就没有国家安全！随着工业化和信息化的融合，越来越多的工控系统开始联入互联网，由于目前工控系统本身的脆弱性，其更容易遭受来自黑客的攻击。

作为业内专业的工控安全厂商，六方云呼吁业界要积极从国内外各个工业安全事件中吸取经验教训，不断完善与丰富工控安全解决方案与服务，加强厂商之间的合作与交流，团结一致，为我国的关键信息基础设施安全贡献力量。